UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	**CASE NO.5:12CR327**
	)	
Plaintiff,	)	**JUDGE CHRISTOPHER A. BOYKO**
	)	
vs.	)	
	)	
JOSEPH J. PIROSKO,	)	**OPINION AND ORDER**
	)	
Defendant.	)	

CHRISTOPHER A. BOYKO, J:

This matter comes before the Court upon Defendant's Motion to Compel Discovery and Request to Extend Pretrial Motion Deadline. (ECF DKT # 26). For the following reasons, Defendant's Motion and Request is denied.

I. BACKGROUND

In July 2012, following a discovery request, the government provided Defendant with various discovery materials and allowed a defense expert, Matthew Curtin of Interhack, to review the computer equipment at issue. On June 25, 2013, Defendant filed the present Motion to Compel Discovery and Request to Extend Pretrial Motion Deadline (ECF DKT # 26). Defendant seeks an Order compelling the government to provide the law enforcement tools and records "used by [Investigator Edward] Sexton to assess information in connection with the particular GUID [Sexton] later associated with [Defendant's] computer equipment."

A GUID, or Globally Unique Identifier, is an "implementation of the universally unique ID that is computed by Windows and Windows applications," which uses "psuedo-random 128-

bit numbers . . . to identify user accounts, documents, software, hardware, software interfaces, sessions, database keys and other items." Relevant to this case, it can be assigned to a computer upon the installation of a peer-to-peer ("P2P") sharing program. On June 4, 2013, Interhack informed the defense that:

> [a]nalysis of the tools used by investigators to create records can determine whether law enforcement officers manipulated data on the subject computer, the error rates in records used, or whether the GUID in question at a particular time is connected to a particular installation of *Limezilla*.

(ECF DKT # 26-1). Interhack explained that it would need access to the records connected to the GUID identified by Sexton and the software used to create those records, in addition to being able to interact with the computers using that GUID. After making the discovery request on June 17, 2013, Defendant had not heard from the government prior to filing this Motion.

The government, in their Response in Opposition to Defendant's Motion to Compel (ECF DKT # 32), explains its reluctance. The tools it used are a part of a broader system of law enforcement surveillance software that, while owned by a private company, is exclusively used by law enforcement officers. The tools used were ShareazaLE, a P2P program, and a database maintained as part of Child Protection Systems ("CPS"), a suite of programs owned by TLO, a private company. ShareazaLE is a modified version of an open-source P2P file sharing system which allows law enforcement to download files exclusively from a target computer. It is "not capable of placing data on a target computer or retrieving data from a target computer, other than the data made publically available by that user." Only specially trained and licensed law enforcement personnel across the world are allowed to use CPS. During such a licensed officer's use of CPS, data is automatically logged onto the CPS database. One of the reasons only specially trained and licensed law enforcement officers are allowed to use the program is to

ensure that any logged data is solely the product of CPS software and law enforcement efforts. The concern is that by letting a defense expert access such software, the integrity of the system would be destroyed, and law enforcement would no longer be able to assure courts that any resulting data is the sole product of the software or law enforcement officers. Further, the expert would have access to a database of information about people currently sharing child pornography.

The government does not indicate whether there are any further tools or records beyond ShareazaLE and CPS programs.

II. LAW AND ANALYSIS

Defendant seeks an Order compelling the government to provide the "law enforcement tools and law enforcement records used by Sexton to assess information in connection with the particular GUID he later associated with [Defendant's] computer equipment." The government has explained that the tools Sexton used are ShareazaLE and the CPS. These programs, the government claims, are sensitive investigatory technologies that are used to track, investigate, and eventually arrest those sharing child pornography through various P2P sharing networks. Because of the sensitive nature of these programs and Defendant's lack of demonstrated need, the Motion to Compel Discovery must be denied.

Defendant believes he is entitled to these law enforcement tools because they were used to assess information connected with the particular GUID later associated with Defendant. Under Fed. R. Crim. P. 16(a)(1)(E), the government:

> must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and:

(i) the item is material to preparing the defense;
(ii) the government intends to use the item in its case-in-chief at trial; or
(iii) the item was obtained from or belongs to the defendant.

The government argues that it is entitled to a qualified privilege based on its interest in maintaining the integrity of its surveillance program. In cases regarding surveillance locations and types, Courts have held that a balance of interests must be weighed to ensure that the public is protected through effective police surveillance systems, while also ensuring the right to a fair trial for defendants. *See*, e.g., *United States v. Gazie*, 1986 WL 16498, at *8-9 (6th Cir. Feb. 26, 1986) ("in some instances, information sought by a defendant may be so critical that his Sixth Amendment right to confrontation would outweigh the government's asserted needs for the privilege"); *United States v. Porter*, 701 F. 2d 1158, 1162-63 (6th Cir. 1983) (refusal to allow defendants to examine surveillance equipment is improper if it deprives defendants of a fair trial). However, even if a defendant may be "hampered to some degree by [the] inability to inspect the surveillance equipment," that does not necessitate the implication of an unfair trial. *Porter*, 701 F. 2d at 1162.

The government has two main concerns. The first relates to the integrity of the surveillance system. For ShareazaLE and CPS to be useful, it is imperative that only specially trained law enforcement officers use the systems. This ensures that when evidence is taken to trial, investigators can assure the courts that only law enforcement and the software contributed to any information the systems provide. Further, the CPS databases are full of information on ongoing investigations into the distribution of child pornography. Allowing the defense expert access to this could compromise those investigations. The second concern is that allowing non-law enforcement individuals to analyze these systems could frustrate future government

surveillance through the programs. The criminals that law enforcement targets via ShareazaLE and CPS are notoriously tech savvy. If given some information on how these systems work criminals could potentially find ways to avoid these surveillance systems. These are exactly the type of considerations that have led to the qualified privilege being applied in other situations. See *United States v. Cintolo*, 818 F. 2d 980, 1002 (1st Cir. 1987) ("discoverability of this kind of [surveillance location] information will enable criminals to frustrate future government surveillance and perhaps unduly jeopardize the security of ongoing investigations"); *United States v. VanHorn*, 789 F. 2d 1492, 1508 (11th Cir. 1986) ("[e]lectronic surveillance is an important tool of law enforcement, and its effectiveness should not be unnecessarily compromised"). The United States has weighty considerations against allowing discovery of these tools, and as will be shown, Defendant will still be able to have a fair trial without access to these tools.

Defendant has proffered three reasons he needs these tools.[1] The first is that it will help determine whether law enforcement officers manipulated data on the Defendant's computer. The government has, however, provided evidence that the ShareazaLE and CPS programs are not capable of manipulating target computers. (Wiltse Aff. ¶ 8). Additionally, the government has provided the logs created when connected to the Defendant's computer and downloaded files. There is nothing to indicate that law enforcement may have, or even could have, manipulated Defendant's computer.

Defendant also seeks the tools to determine the error rates in the records used. To be able

[1]These reasons have been inferred from the quoted portion of the email from Matthew Curtin of Interhack (ECF DKT 26-1) found on page two of Defendant's Motion to Compel Discovery and Request to Extend Pretrial Motion Deadline (ECF DKT # 26).

to determine the function of the application and validate its calibration, however, the defense expert would need the source code. (Wiltse Aff. ¶ 10). This source code is in the exclusive possession of TLO, and has never been given to law enforcement. A government is not responsible for producing that which was never in its control. *United States v. Sepulveda*, 15 F. 3d 1161, 1179 (1st Cir. 1993); *United States v. Hughes*, 211 F. 3d 676, 688 (1st Cir. 2000); *United States v. Friedman*, 593 F. 2d 109, 119-20 (9th Cir. 1979); *United States v. Flores*, 540 F. 2d 432, 437-38 (9th Cir. 1976). The government has stated it would be willing to offer expert testimony at an evidentiary hearing on the error rate. Such testimony, if from someone such as Wiltse, would address the issue without risking the integrity of the surveillance system. This type of testimony on a very similar program was seen as satisfactory for purposes of the *Daubert* rule. See *United States v. Chiaradio*, 684 F. 3d 265, 276-78 (1st Cir. 2012) (cert. denied). Defendant does not need the programs to determine its error rates in order to receive a fair trial.

The third inferred reason Defendant seeks the tools is to determine "whether the GUID in question at a particular time is connected to a particular installation of *Limezilla*." The Court is not entirely clear why the defense expert requires the tools for this purpose. The defense expert had access to Defendant's computer, which, according to the government, should provide any information the defense needs about the computer's GUID. ShareazaLE and CPS only record the GUID of the target computer and log that information onto a database. Moreover, according to the government, the importance of the GUID is not necessarily that it is entirely unique.[2] Instead, the significance of the GUID is that it was "traced to several locations from which child

[2]The government admits that there is a possibility it was not unique. They point out, however, that the odds are "astronomical" for a 32 alphanumeric digit long GUID to be assigned to another computer that was also sharing child pornography.

pornography files were shared and at which Defendant was confirmed to have been on the dates and times in question." Thus, this final concern is also not enough to require the Court to compel the government provide the defense expert with the software. *Compare* with *Gazie*, 786 F. 2d 1166 (finding a qualified privilege where defendant sought to show microphones were in boxes, which could distort voice identification, but defendants were identified by other means aside from voice).

This case is also distinguishable from *United States v. Budziak*, 697 F. 3d 1105 (9th Cir. 2012). In *Budziak*, the Defendant sought the discovery of very similar software that was used in the investigation of the distribution of child pornography. The Ninth Circuit held that the Defendant should have been able to assess this software because:

> Budziak presented evidence suggesting that the FBI may have only downloaded fragments of child pornography files from his "incomplete" folder, making it "more likely" that he did not knowingly distribute any complete child pornography files . . . . Budziak [also] submitted evidence suggesting that the FBI agents could have used the EP2P software to override his sharing settings.

Id. at 1112. In the present case there is no evidence from Defendant that would indicate anything comparable occurred. Indeed, as mentioned, the government has offered evidence that the ShareazaLE and CPS are *not* capable of overriding sharing settings. Without any reason to believe the programs are necessary for the defense, there is no reason to deny the qualified privilege that the ShareazaLE and CPS programs are entitled to.

At a later point, an evidentiary or ex parte hearing may be appropriate to fully determine whether Defendant should be able to access the software. Many similar cases have required such a hearing, and indeed, in *Gazie*, the Sixth Circuit noted that the record created by the trial judge through conducting an ex parte, in camera hearing and specifically listing the factors underlying the decision in favor of the government was "critical" to its review. 786 F. 2d 1166 (Footnote

14). The Sixth Circuit went on to "urge all trial judges faced with such an issue to conduct themselves in a similar fashion. *Id.* At this time, however, Defendant has not shown it needs ShareazaLE and the CPS in order to receive a fair trial.

III. CONCLUSION

For the foregoing reasons, the Court DENIES Defendant's Motion to Compel Discovery and Request to Extend Pretrial Motion Deadline (ECF DKT # 26).

IT IS SO ORDERED.

s/ Christopher A. Boyko
CHRISTOPHER A. BOYKO
United States District Judge

Dated: August 13, 2013